

CLAIMS

What is claimed is:

1. A method, comprising the steps of:

receiving a record;

5 referencing a set of access rules for the record; and

applying an appropriate set of access rules to limit access to the record, the limitations being enforced one or more selected from the group consisting of a cryptographic method for selectively limiting record access based on possession of a cryptographic key, and a trustee applying the access rules to limit access to the record.

10 2. The method according to claim 1, further comprising the step of accounting for a decryption of the record.

3. The method according to claim 2, wherein said accounting is anonymous.

15 4. The method according to claim 1, wherein the record has a plurality of portions, each portion being encrypted with at least one cryptographic key, said portions being independently accessible, said access rules applying to selectively limit access to portions of the record.

20 5. The method according to claim 4, wherein said access rules limit access to portions based on an identity of an intended recipient.

6. The method according to claim 1, further comprising the step of supplying a decryption key for a respective record portion in accordance with the applied set of rules.

7. The method according to claim 1, further comprising the step of accounting for a decryption of a portion of the record.

8. The method according to claim 1, wherein the set of access rules are associated with an intended recipient of the record.

9. The method according to claim 1, further comprising the step of referencing an index to define a record.

10. The method according to claim 9, wherein the index further stores a set of access rules for qualifying an intended recipient with respect to each of the records.

5 11. The method according to claim 1, further comprising the step of using an index to identify a record potentially responsive to a query.

12. The method according to claim 1, further comprising the step of using an index comprising a set of associations of patient identities and medical transaction records to identify records relating to a respective patient.

10 13. The method according to claim 1, further comprising the step of using an index comprising a set of associations of record identification, record characteristic, and said access rules to identify records relating to a query and limiting access to portions thereof.

14. The method according to claim 1, wherein the record comprises a plurality of portions, the portions being separately encrypted and having associated sets of independent rules.

15. The method according to claim 1, wherein the access rules are role based access rules relating to a role of the intended recipient.

16. The method according to claim 1, wherein the access rules are context based access rules relating to a context of record access.

17. The method according to claim 1, wherein the access rules are defined by a rights-
20 holder of the record.

18. The method according to claim 1, wherein a decryption of the record triggers a remotely-sensed transaction.

19. The method according to claim 18, wherein the remotely sensed transaction comprises a financial accounting transaction.

20. The method according to claim 18, wherein the remotely sensed transaction comprises an access audit trail transaction.

21. The method according to claim 2, wherein said accounting occurs upon supply of the respective decryption key.

5 22. The method according to claim 2, wherein said accounting occurs upon use of the respective decryption key.

23. The method according to claim 1, wherein the record comprises a medical record.

24. The method according to claim 1, wherein the record comprises a media content record.

10 25. The method according to claim 1, wherein the access rules comprise a database of jurisdictional trust laws.

26. The method according to claim 1, wherein the set of access rules comprises a database of jurisdiction-dependent privacy laws.

15 27. The method according to claim 1, further comprising the step of creating a virtual trust of the record implemented in accordance with the trust laws of an associated jurisdiction.

20 28. The method according to claim 1, wherein the records comprise separate articles within a digital publication.

29. The method according to claim 1, further comprising the step of receiving the set of access rules.

30. The method according to claim 1, further comprising the step of generating the set of access rules based on the record.

31. The method according to claim 1, wherein a record encryption is associated with a rolling code.

32. The method according to claim 1, wherein the trustee controls the records and implements the access rules without requiring access to a content of the record.

33. The method according to claim 1, wherein the trustee controls access to the records.

5 34. The method according to claim 1, wherein the trustee selectively processes the records.

35. The method according to claim 1, wherein the records comprise a type selected from the group consisting of legal information, government records, financial records, commercially valuable trade secret legal information, manufacturing information, banking information, consumer entertainment media, digital music files, video information, cinema information, consumer information, personal demographic information, credit card information, personal contact information, social security number information, publication information, separate articles within a digital publication, and investment account information.

36. The method according to claim 1, wherein the record comprises a patient file, placed in a privileged trust for the patient with an independent trustee, said trustee implementing the set of rules for access with respect to each transaction record within the patient file defined by the patient and legal jurisdiction, wherein said trustee interacts with the patient record information to maintain, process, receive, deliver, or transmit portions of the patient record in secure and verifiable fashion to authorized entities in compliance with the trust.

20 37. The method according to claim 1, wherein the record comprises a corpus of a medical information trust for holding medical records on behalf of patients, in an organization distinct from the caregiver; the trustee charging for access to the medical record, and maintaining a record of each access of the medical record.

25 38. The method according to claim 1, wherein access rules are applied to an identified intended recipient without communicating an identity of the intended recipient to the respective beneficiary.

39. A method, comprising the steps of:

placing information in trust with a trustee on behalf of a beneficiary;

permitting a user to access the information in the trust; and

implementing a rule for selectively providing access to the information in trust, including requiring an electronic communication between the user and the trustee.

5 40. The method according to claim 39, wherein the rule comprises a compensation rule for obtaining a right to the information.

 41. The method according to claim 40, wherein the electronic communication comprises an electronic funds transfer.

 42. The method according to claim 40, wherein the compensation rule is integrally associated with the information, and wherein the implementing occurs as a result of user interaction with the information.

 43. The method according to claim 39, wherein the information comprises a patient medical record.

 44. The method according to claim 39, wherein the information comprises consumer entertainment media.

 45. The method according to claim 39, wherein the trustee is interposed between a rights holder for the information and the user, the trustee maintaining an anonymity of the user while accounting to the rights holder.

20 46. The method according to claim 39, wherein the trustee is interposed between a rights holder for the information and the user, the trustee characterizing the user based on a classification of information usage, while accounting to the rights holder for the use, without specifically identifying information usage of a user.

 47. The method according to claim 39, wherein a transfer of the information to the user requires an electronic transfer of value from the user to the trustee, further comprising the

step of accepting the value by the trustee while stripping a retained transfer record of an identifier of the user.

48. The method according to claim 39, further comprising the steps of receiving an identification of desired information content from a user; and logging the access employing a digital signature of the user.

49. The method according to claim 48, wherein the digital signature is anonymous with respect to the beneficiary.

50. The method according to claim 48, wherein the permitting the access entails requiring the user to enter into a restrictive covenant.

51. The method according to claim 40, wherein the trustee manages access to the information and implements the access rules as an intermediary for, and communicates compensation information to, the beneficiary.

52. The method according to claim 40, wherein the information has an associated compensation value, and comprises digital media information, said digital media information being associated with subsidy content, further comprising the step of accounting with the user for use of the digital media information offset by a value for subsidy content.

53. A method, comprising the steps of:

defining information content and associated access rules; transmitting the information content and associated access rules to a trustee; and

implementing, by the trustee, the associated access rules with respect to the information content, to establish a virtual trust in accordance therewith.

54. The method according to claim 53, wherein the information content comprises media information, and the associated access rules comprise economic rules.

55. The method according to claim 53, wherein the information content comprises medical record information, and the associated access rules comprise restrictive access rules based on an identity or characteristic of the user.

56. The method according to claim 55, further comprising the step of transmitting,
5 from the trustee, information content in accordance with the associated rules.

57. The method according to claim 53, wherein the trustee controls the information content and implements the rules without requiring access to the information content.

58. A database system, comprising a plurality of records, each record having an associated set of access rules, means for applying the appropriate set of access rules to limit
10 access to the record, the limitations being enforced by one or more selected from the group consisting of a cryptographic method for selectively limiting record access based on possession of a cryptographic key and a trustee applying the access rules on behalf of a beneficiary.

59. The system according to claim 58, further comprising means for accounting for a decryption of the record.

60. The system according to claim 59, wherein said accounting is anonymous.

61. The system according to claim 58, wherein the record has a plurality of portions, each portion being encrypted with at least one cryptographic key, said portions being independently accessible, said access rules applying to selectively limit access to portions of the record.

20 62. The system according to claim 61, wherein said access rules limit access to portions based on an identity of an intended recipient.

63. The system according to claim 58, further comprising the step of supplying a decryption key for a respective record portion in accordance with the applied set of rules.

64. The system according to claim 58, further comprising an accounting system for
25 accounting for a decryption of a portion of the record.

65. The system according to claim 58, wherein the set of access rules are associated with an intended recipient of the record.

66. The system according to claim 58, further comprising the step of referencing an index to define a record.

5 67. The system according to claim 66, wherein the index further stores a set of access rules for qualifying an intended recipient with respect to each of the records.

68. The system according to claim 67, further comprising the step of using an index to identify a record potentially responsive to a query.

69. The system according to claim 58, wherein an index of a set of associations of patient identities and medical transaction records is used to identify records relating to a respective patient.

70. The system according to claim 58, wherein an index of a set of associations of record identification, record characteristic, and said access rules to identify records relating to a query and limiting access to portions thereof.

71. The system according to claim 58, wherein the record comprises a plurality of portions, the portions being separately encrypted and having associated therewith sets of independent rules.

72. The system according to claim 58, wherein the access rules are role based access rules relating to a role of the intended recipient.

20 73. The system according to claim 58, wherein the access rules are context based access rules relating to a context of record access.

74. The system according to claim 58, wherein the access rules are defined by a rights-holder of the record.

25 75. The system according to claim 58, wherein a decryption of the record triggers a remotely-sensed transaction.

76. The system according to claim 75, wherein the remotely sensed transaction comprises a financial accounting transaction.

77. The system according to claim 75, wherein the remotely sensed transaction comprises an access audit trail transaction.

5 78. The system according to claim 59, wherein said accounting occurs upon supply of the respective decryption key.

79. The system according to claim 59, wherein said accounting occurs upon use of the respective decryption key.

80. The system according to claim 58, wherein the record comprises a medical record.

81. The system according to claim 58, wherein the record comprises a media content record.

82. The system according to claim 58, wherein the access rules comprise a database of jurisdictional trust laws.

83. The system according to claim 58, wherein the set of access rules comprises a database of jurisdiction-dependent privacy laws.

84. The system according to claim 58, further comprising the step of creating a virtual trust encompassing the record, implemented in accordance with the trust laws of an associated jurisdiction.

85. The system according to claim 58, wherein the records comprise separate articles
20 within a digital publication.

86. The system according to claim 58, further comprising the step of receiving the set of access rules.

87. The system according to claim 58, further comprising the step of generating the set of access rules based on the record.

88. The system according to claim 58, wherein a record encryption is associated with a rolling code.

89. The system according to claim 58, wherein the trustee controls the records and implements the access rules without requiring access to a content of the record.

90. The system according to claim 58, wherein the trustee controls access to the records.

91. The system according to claim 58, wherein the trustee selectively processes the records.

92. The system according to claim 58, wherein the records comprise a type selected from the group consisting of legal information, government records, financial records, commercially valuable trade secret legal information, manufacturing information, banking information, consumer entertainment media, digital music files, video information, cinema information, consumer information, personal demographic information, credit card information, personal contact information, social security number information, publication information, separate articles within a digital publication, and investment account information.

93. The system according to claim 58, wherein a record comprises a patient file, placed in a privileged trust for the patient with an independent trustee, said trustee implementing the set of rules for access with respect to each transaction record within the patient file, said rules being defined by the patient and legal jurisdiction, wherein said trustee interacts with the patient record information to maintain, process, receive, deliver, or transmit portions of the patient record in secure and verifiable fashion to authorized entities in compliance with the trust.

94. The system according to claim 58, wherein a record comprises a corpus of a medical information trust for holding medical records on behalf of patients, in an organization distinct from the caregiver; the trustee charging for access to a medical record, and maintaining a record of each access of said medical record.

95. The system according to claim 58, wherein access rules are applied to an identified intended recipient without communicating an identity of the intended recipient to the respective beneficiary.

96. A system, comprising:

5 a trust, formed by providing information to a trustee on behalf of a beneficiary along with a set of access rules to be applied by the trustee to selectively permit a user to access the information in the trust; and

means for automatically providing selective access to the information, in accordance with the set of access rules, based on an electronic communication between the user and the trustee.

10 97. The system according to claim 96, wherein the rule comprises a compensation rule for obtaining a right to the information.

98. The system according to claim 97, wherein the electronic communication comprises an electronic funds transfer.

15 99. The system according to claim 97, wherein the compensation rule is integrally associated with the information, and wherein the implementing occurs as a result of user interaction with the information.

20 100. The system according to claim 96, wherein the information comprises a patient medical record.

101. The system according to claim 96, wherein the information comprises consumer entertainment media.

102. The system according to claim 96, wherein the trustee is interposed between a rights holder for the information and the user, the trustee maintaining an anonymity of the user while accounting to the rights holder.

25 103. The system according to claim 96, wherein the trustee is interposed between a rights holder for the information and the user, the trustee characterizing the user based on a

classification of information usage, while accounting to the rights holder for the use, without specifically identifying information usage of a user.

104. The system according to claim 96, wherein a transfer of the information to the user requires an electronic transfer of value from the user to the trustee, further comprising the step of accepting the value by the trustee while stripping a retained transfer record of an identifier of the user.

105. The system according to claim 96, further comprising means for receiving an identification of desired information content from a user; and means for logging the access employing a digital signature of the user.

106. The system according to claim 105, wherein the digital signature is anonymous with respect to the beneficiary.

107. The system according to claim 96, wherein the user is required to enter into a restrictive covenant for access to the information.

108. The system according to claim 97, wherein the trustee manages access to the information and implements the access rules as an intermediary for, and communicates compensation information to, the beneficiary.

109. The system according to claim 97, wherein the information has an associated compensation value, and comprises digital media information, said digital media information being associated with subsidy content, wherein the user accounts to said selective access providing means for use of the digital media information offset by a value for subsidy content.

110. A virtual trust system, comprising a set of defined information content and associated rules; and

a trustee, receiving the information content and associated rules and implementing a virtual trust in accordance therewith.

111. The system according to claim 110, wherein the information content comprises media information, and the associated access rules comprise economic rules.

112. The system according to claim 110, wherein the information content comprises medical record information, and the associated access rules comprise restrictive access rules based on an identity or characteristic of the user.

113. The system according to claim 112, further comprising the step of transmitting,
5 from the trustee, information content in accordance with the associated rules.

114. The system according to claim 110, wherein the trustee controls the information content and implements the rules without requiring access to the information content.

115. The system according to claim 110, wherein the defined information content is provided as a set of records, each record having a plurality of portions, at least two such portions
10 being associated with independent cryptographic keys, further comprising a database index providing an association between a record descriptor, a record identification, and a set of limiting access rules for each privileged database record; and a cryptographic key database, for storing cryptographic keys associated with portions of a record.

116. The system according to claim 110, wherein said rules are selected from the group
15 consisting of role based access rules, and context based access rules.

117. The system according to claim 115, wherein each of the portions is encrypted with at least one cryptographic key, said portions being independently accessible.

118. The system according to claim 115, further comprising means for accounting for a decryption of an encrypted record or portion of a record.

20 119. The system according to claim 115, wherein the records comprise medical records.

120. The system according to claim 110, wherein the set of rules comprise a database of jurisdictional trust laws.

121. The system according to claim 110, wherein the rules are jurisdiction-dependent,
25 further comprising an input for receiving an identification of a relevant jurisdiction.

122. The system according to claim 121, further comprising means for resolving inconsistencies between a plurality of relevant jurisdictions.

123. The system according to claim 121, further comprising a plurality of rule sets, each rule set being associated with a different jurisdiction, further comprising means for applying
5 a set of rules relevant to an associated jurisdiction.

124. The system according to claim 110, further comprising a transaction log including a digital signature of a transactor, wherein the transaction log may be audited through use of a complementary digital signature.

125. The system according to claim 124, wherein the transaction log may be audited
10 without revealing an identity of the transactor.

126. The system according to claim 124, wherein the transaction log audited reveals an identity of the transactor.

127. A transmitted medical information record, including patient-specific data, comprising at least one medical transaction information file, associated with the specific patient, each medical transaction information file being separately encrypted.

128. The record according to claim 125, wherein the record comprises at least two medical transaction information files, each file being separately encrypted.

129. The record according to claim 125, further comprising an access rule embedded in the medical transaction information file.

130. The record according to claim 125, wherein the access rule is not encrypted.
20

131. The record according to claim 125, wherein the medical transaction file encryption comprises public key encryption.

132. The record according to claim 125, wherein the medical transaction file encryption comprises multiple levels of public key encryption, employing differing keys.

133. The record according to claim 125, wherein the medical transaction file encryption comprises a first public key encryption employing a patient-specific public key, and a second public key encryption employing a recipient specific public key.

134. The record according to claim 125, wherein the medical transaction file encryption comprises a public key encryption employing a recipient-system interaction specific key.

135. The record according to claim 134, wherein the medical transaction file encryption further comprises a first public key encryption employing a patient-specific public key, and a second public key encryption employing a recipient specific public key.

136. The record according to claim 134, wherein said recipient-system interaction specific key interacts with an applet wrapper to decrypt the medical record.

137. A system for managing the record according to claim 125, comprising a database system for hosting the medical transaction information files, and an accounting system for accounting for access to a content of each of said encrypted medical transaction information files.

138. The system according to claim 137, wherein the accounting is a financial accounting.

139. The system according to claim 137, further comprising an audit trail.

140. A business method, comprising the steps of:

establishing, in an organization distinct from the caregiver, a medical information trust to hold a medical record or associated access permission on behalf of a patient;

charging for access to or permission to access the medical record; and

maintaining a record of each access of or permission to access the medical record.

141. The method according to claim 140, wherein the access permission comprises a cryptographic key.

142. A business method, comprising the steps of:

establishing, in an organization distinct from a rights holder, a virtual information trust to hold a content record or associated access permission on behalf of a rights holder;

charging for access to or permission to access the content record; and

5 maintaining a record of each access of or permission to access the content record.

143. The method according to claim 142, wherein the access permission comprises a cryptographic key.

TESE "434333"